Cloud Security

혁신적인 악성코드 선제 방어 기술로 더욱 안전한 Microsoft 365 구현

Microsoft 365로 유입되는 피싱 이메일, 랜섬웨어,
이메일 사기 공격(BEC)으로부터 사용자를 보호합니다.

DISARM

CONTENT SECURITY for Email

Challenge

전체 사이버 공격 중 이메일을 통해 감행되는 지능형 보안 위협은 75%이며, 이 중 72%의 공격이 비실행 파일(문서) 이용

비실행 파일(문서) 기반 알려지지 않은 잠재 보안 위협까지 실시간으로 선제 차단 (예: Hyperlink, Visual Basic Macro, JavaScript, Dynamic Data Exchange 등)

Solution

기존 이메일 보안 서비스는 끊임없이 진화하는 위협 환경에서 시그니처 기반 방어에 의존

혁신적인 DISARM은 제로 트러스트 기반 콘텐츠 무해화(CDR)과 악성코드 선제 방어 기술(디버거 기술)로 Microsoft 365 이메일 사용자 및 콘텐츠 보호

몇 분 안에 Microsoft 365 Mail과 쉽고 빠르게 연동되며, 서비스 통합 관리가 가능한 완전한 SaaS 솔루션

DISARM은 Microsoft 365의 기본 보안 기능을 보완해 알려지지 않은 위협까지 대응하는 제로 트러스트 기반 통합 클라우드 이메일 보안 서비스입니다.

최근 기업 정보를 노리는 공격은 날이 갈수록 고도화되고 있습니다. 공격자들은 이메일을 공격 수단으로 사용하기 때문에 업무 문서로 위장한 악성 메일이 유입될 경우 선제 대응이 어렵습니다.

디지털 전환으로 협업 소프트웨어 사용이 크게 증가함에 따라 이메일은 비즈니스를 위한 중요한 커뮤니케이션 수단이 되었습니다. 전체 사이버 공격 중 이메일을 통해 감행되는 지능형 보안 위협은 75%이며, 이 중 72%가 비실행 파일(문서)이용한 공격입니다.

특히, 최근 비실행 파일 악성코드는 사용자 행위가 있어도 바로 실행되지 않고 특정 시간이 지난 이후에 실행되거나, 특정 행위에만 반응하는 등 비정형적인 패턴을 보이고 있어 이에 대한 대응이 쉽지 않습니다. 침투한 악성코드 흔적을 이전의 데이터베이스와 비교해 진단하는 시그니처 보안 솔루션으로는 즉각적인 대응이 어렵기 때문입니다.

DISARM은 이메일로 유입되는 알려진 보안 위협뿐만 아니라 알려지지 않은 보안까지 빠르고 정확하게 탐지·진단하기 때문에 Microsoft 365가 제공하는 보안 기능만으로는 차단이 어려운 '지능형 보안 위협'에 효과적으로 대응합니다.

독보적인 위협 인텔리전스(TI), 디버거 분석, 콘텐츠 무해화(CDR) 기술이 결합된 콘텐츠 샌드박스를 통해 Microsoft 365 사용자에게 더욱 안전한 이메일 서비스를 제공합니다.

Microsoft 365는 이미 알려진 보안 위협은 잘 차단하지만 알려지지 않은 보안 위협까지 방어하기 어렵습니다.

DISARM은 Microsoft 365를 우회하는 고도화된 지능형 보안 위협까지 차단하여 Microsoft 365의 보안을 강화합니다.

SECULETTER

최근 악성코드 침해 현황

최근 사이버 위협이 고도화되면서 '문서'를 통해 공격을 가하는 해킹 사례가 늘고 있습니다. 악성코드 공격의 상당수는 이메일을 통해 발생합니다. 특히 이메일 내 악성코드의 대부분은 첨부문서 파일로 위장하여 진단이 매우 어렵습니다.

비즈니스 이메일 해킹 시도 건수

3500만 annual

156,000 daily

※ 출처 : MS 사이버 위협 보고서 2023

악성 URL 피싱 공격 건수

417,678

※ 출처 : MS 사이버 위협 보고서 2023

악성 첨부문서 기반 공격 비중

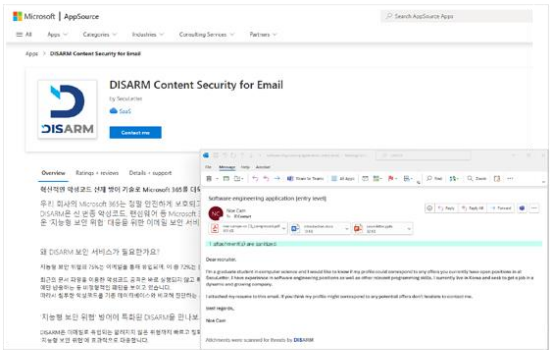
97.1%

※ 출처 : 2022~2023 시큐레터 데모 신청 고객 기준

제로 트러스트 기반 강력한 위협 대응

제로 트러스트 기반 콘텐츠 무해화(CDR) 기술로 첨부문서 내 악성 URL, 자바스크립트, 쉘코드 등 액티브 콘텐츠를 제거해 잠재적 위협 요소까지도 강력하게 대응합니다.

- 이메일과 첨부파일에서 유해 컨텐츠 제거 후, 원본 파일 손상을 최소화하여 재조합
- 파일을 통한 랜섬웨어 등의 보안 위협이 사용자 이메일 시스템에 침투하는 것을 예방



[제로 트러스트 기반 콘텐츠 무해화(CDR) 적용 화면]

알려지지 않은 공격까지 선제 차단

독보적인 콘텐츠 샌드박스(디버거 분석 + 콘텐츠 무해화)를 통해 알려진 보안 위협 뿐만 아니라 Microsoft 365 기본 보안 기능을 우회하는 알려지지 않은 보안 위협도 정확하고 빠르게 탐지하며 사용자의 이메일 열람 전에 차단합니다.

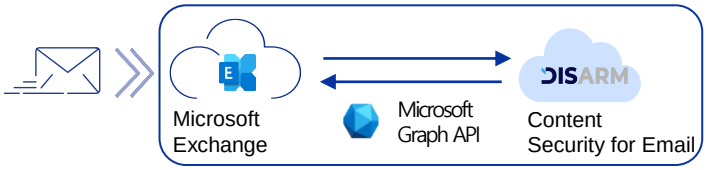
- 시그니처가 없는 알려지지 않은 보안 위협 탐지
- 탐지를 회피하는 보안 위협 탐지
- 정교한 해킹 공격에도 강력한 방어 기능 제공

[디버거 분석(자동화된 리버스 엔지니어링) 과정]

Microsoft 365와의 빠르게 연동되는 클라우드 기반 서비스 (ICES: Integrated Cloud Email Security)

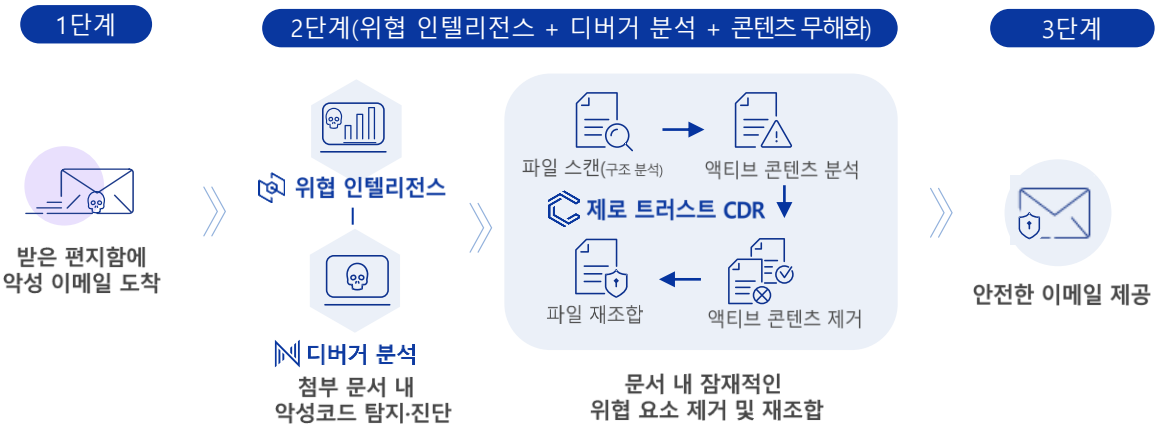
Microsoft 365 계정과 5분 안에 연동되어 효율적인 서비스 통합 관리가 가능합니다.

- 구독 시 MX 레코드 값 변경 없이 Microsoft 365와 쉽고 빠르게 연동(MS API 활용)
- 구조적으로 이메일 유실 없는 안정적인 서비스 제공
- 조직 내부에서 주고 받는 이메일도 안전하게 보호
- 관리자 웹을 통해 편리한 서비스 통합 관리 가능



[DISARM과 Microsoft 365 연동 과정]

주요 기능



수신된 이메일에 대한 신.변종 보안 위협 선제 차단 과정

악성코드 차단
실행 파일 및 비실행 파일 등 다양한 파일의 악성코드, 랜섬웨어 탐지 및 진단

악성 URL 차단
악성 첨부 파일 및 본문 내 악성 URL 등 보안 위협 진단 및 차단

콘텐츠 무해화(CDR)
문서 내 악성 액티브 콘텐츠 선제 제거 후원본에 가깝게 재구성 (doc/docx/docm/rtf, xls/xlsx, ppt/pptx/pptm, pdf, 이미지 파일 등 지원)

압축 파일의 악성코드 차단
압축파일 전체를 스캔하여 악성코드 여부 검사 (ZIP, 7Z, ARJ, RAR, TGA 등 지원)

암호화된 문서의 악성코드 탐지
암호화된 문서 내 악성 여부 진단 후 위협 요소 차단

이메일 피싱 공격 차단
첨부된 악성 파일 식별하여 이메일 피싱 공격 탐지 및 차단

이메일 프로파일링 제공
최근 이메일 수·발신 기록이 없는 발송인의 경우 수신자에게 위험성 알림

조직 내 이메일 송·수신 보안
조직 내부에서 주고 받는 이메일에 대한 보안 강화

관리자 페이지 제공
기업 내 구매 및 IT 담당자가 실시간으로 기업의 메일 흐름을 파악할 수 있는 관리자 페이지 제공

다양한 정책 지원
이메일 첨부 파일, 이메일 본문 내 URL, 첨부 파일 내 URL 등 기업의 필요에 따라 정책 설정 가능

VIP 메일 정보 마스킹 지원
내부 중요 사용자의 수신 메일 정보를 마스킹하여 민감 정보 보호

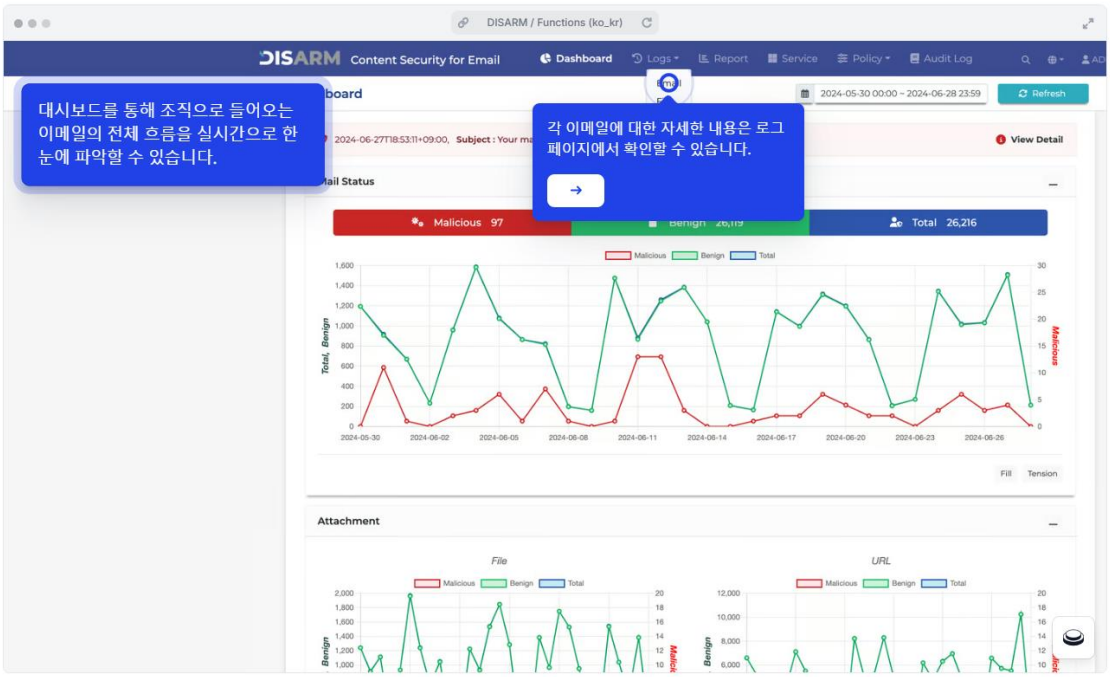
콘텐츠 보안 전문 TI 지원
콘텐츠 기반 다양한 정보 관리로 보안 위협에 빠르게 대응하는 위협 인텔리전스 제공

콘텐츠 기반 보안 위협 상세 정보 제공
악성코드 분석 전문가를 위한 비실행(Non-PE) 파일 상세 분석을 통해 보안 위협에 대한 자세한 정보 제공

신·변종 보안 위협 차단
리버스 엔지니어링 기반 디버거 분석 통해 known과 Unknown 보안 위협 탐지/차단

월간 리포트 작성
31일 간격 주기로 이메일 흐름을 한 눈에 파악할 수 있도록 보고서 생성 기능 제공

제품 체험 하기



[체험하기] https://www.seculetter.com/cloud-security.php

요금제 및 가격

DISARM으로 Microsoft 365 이메일 서비스를 더욱 안전하게 사용하세요!
지금 구매하시면 **첫 30일을 무료로** 사용할 수 있습니다.

BASIC

$36.00

Per user/year

- 악성코드 분석
- 보안 위협 요소 탐지· 차단
- 첨부파일 악성 여부 진단
- 콘텐츠 보안 전문 TI 지원
- 이메일 피싱 공격 차단

지금 구매

STANDARD

★ 제로트러스트 CDR 지원

$42.00

Per user/year

- BASIC 기능
- 문서 내 악성 액티브 콘텐츠 선제 제거 & 파일 재구성(CDR)
- 파일 공유 시 발생하는 보안 위협 사전 예방

지금 구매

ADVANCED

★ 콘텐츠 샌드박스 지원

$60.00

Per user/year

- STANDARD 기능
- 알려지지 않은 보안 위협 차단 (디버거 분석)
- 콘텐츠 기반 상세 위협 정보 제공 (악성코드 전문가용 상세 분석)
- 이메일 프로파일링

지금 구매

FAQ's

DISARM 서비스를 설치하면 Microsoft 365 에 제로 트러스트 CDR 이 어떻게 적용되나요?

구독자가 수신한 이메일은 DISARM 서비스가 먼저 악성 여부 분석 및 첨부파일 무해화 과정 수행 후 안전한 메일로 변경하여 Microsoft 365 받은편지함으로 전달합니다. 구독자는 메일 본문 상단 알림바를 통해 콘텐츠 무해화가 완료되었음을 알 수 있으며, 악성 이메일의 수신될 경우 DISARM 에서 격리시킨 후 탐지 결과를 사용자에게 알림 메일로 안내합니다.

DISARM 서비스를 이용하려면 어떻게 해야 하나요?

Microsoft 앱 소스 'DISARM' 페이지에서 원하는 구독 플랜을 선택하시면 서비스를 바로 이용할 수 있습니다. 자세한 내용은 Microsoft 앱 소스 'DISARM' 페이지 참고 바랍니다.

조직에 이미 Microsoft 365 보안이 있는 경우 어떻게 해야 하나요?

계정 탈취 목적을 가진 최신 악성 피싱 이메일 탐지 사례가 있습니다. Microsoft 365는 해당 메일을 정상으로 판별하여 메일 수신함으로 보냈지만 DISARM은 악성으로 탐지하여 메일 수신함에 메일이 수신되기 전에 차단했습니다.

Microsoft 365에서는 탐지하지 못하고 DISARM 에서만 탐지한 사례가 있나요?

계정 탈취 목적을 가진 최신 악성 피싱 이메일 탐지 사례가 있습니다. Microsoft 365는 해당 메일을 정상으로 판별하여 메일 수신함으로 보냈지만 DISARM은 악성으로 탐지하여 메일 수신함에 메일이 수신되기 전에 차단했습니다.

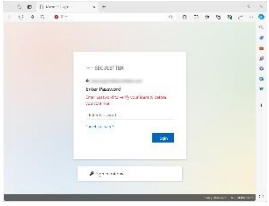
조직에 이미 Microsoft 365 보안이 있는 경우 어떻게 해야 하나요?

Microsoft 365에서 제공하는 보안 솔루션이 있더라도 조직의 보안 강화를 위해 DISARM 도입을 추천합니다. Microsoft 365 의 보안 기능은 시그니처 기반 보안(예: Anti-Virus, SPAM 등)을 제공하기 때문에 보안 기능을 우회하는 '알려지지 않은 신·변종 악성코드/랜섬웨어(Unknown Threat)'가 유입될 경우 탐지·차단이 어렵습니다. 이와 달리 DISARM은 알려진 보안 위협뿐만 아니라 알려지지 않은 보안 위협까지도 독자적인 리버스 엔지니어링 기술을 통해 모두 탐지해 선제 차단합니다. 또한 콘텐츠 무해화 기술을 통해 모든 비즈니스 콘텐츠(MS Office, HWP, PDF, JPG, PNG 등)를 사이버 공격이 불가능하도록 무해화 시키기 때문에 더욱 안전한 Microsoft 365를 사용할 수 있습니다.

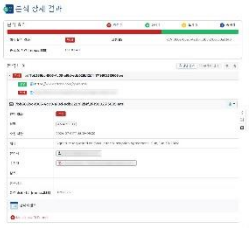
Microsoft 365에서 제공하는 추가적인 보안 강화 서비스 구독 대신 DISARM을 선택해야 하는 이유는 무엇입니까?

Microsoft 365 에서 제공하는 별도의 보안 서비스 'Office 365용 Microsoft Defender Plan 1 / Plan 2' 을 추가로 구독하면, 더욱 향상된 피싱 탐지 및 다양한 보안 기능이 제공됩니다. 하지만 Microsoft에서 제공하는 보안 기능은 DETECT(탐지) 방식 위주로 구성되어 있습니다. 이는 최신 변종 해킹 공격을 탐지하지 못할 수 있습니다. 반면에 시큐레터는 이메일 보안 전문 기업으로서 제로 트러스트 철학을 반영한 보안을 제공하기 때문에 DISARM은 해킹 및 피싱 공격 원천 방어에 특화되어 있습니다.

[그림 1]
악성 피싱 메일 원본



[그림 2] 악성 피싱 메일의 URL 클릭 시 보여지는 계정 탈취용 페이지



[그림 3] DISARM 탐지 화면